UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

MEYER GELFMAN, BORIS PARAD, and YELENA PARAD, individually and on behalf of all others similarly situated, Plaintiffs, v. **ILLINOIS GASTROENTEROLOGY GROUP, P.L.L.C.,** Defendant.	Case No. 1:22-cv-05006 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs MEYER GELFMAN, BORIS PARAD, and YELENA PARAD, individually, and on behalf of all others similarly situated ("Plaintiffs"), through their undersigned attorney, bring this action against Defendant Illinois Gastroenterology Group, P.L.L.C. ("Defendant") and allege upon personal knowledge as to their own actions and experiences, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Defendant solicited, collected, digitized, aggregated, stored, and failed and refused to protect approximately 227,943 of its patients' sensitive personally identifiable and health information from known cyber threats, including their name, address, date of birth, Social Security number, driver's license, Passport, financial account information, payment card information, employer-assigned identification number, medical information, and biometric data ("PII/PHI").

2. Defendant failed to comply with regulatory, ethical, and industry standards for cybersecurity and confidentiality of patient records, failed to take the most basic security measures

such as encryption of data and destruction of obsolete data, and failed to prevent, detect, and adequately respond to a foreseeable data breach carried out by cyber criminals. As a result, criminals gained access to, copied, and stole Plaintiffs' and Class members' PII/PHI (the "Data Breach").

3. Although Defendant learned of the Data Breach on or before November 18, 2021, it unreasonably delayed notifying Plaintiffs and Class members for 5 months, giving the criminals a head start to commit identity fraud, theft, and wreak havoc to Plaintiffs' and Class members' personal finances, identities, and accounts.

4. After an unreasonably long silence, on April 22, 2022, Defendant sent letters to Plaintiffs and Class members notifying them of the Data Breach and provided the legally required notification to the authorities.

5. As a direct result of the Data Breach, Plaintiffs and Class members have suffered numerous actual and concrete injuries and will suffer additional injuries into the future. Plaintiffs seek damages and other legal and equitable relief for the following categories of harms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (d) loss of time and loss of productivity heeding Defendant's warnings and following its instructions in Defendant's notice letter; (e) financial costs incurred due to actual identity theft; (f) the cost of future identity theft monitoring; (g) loss of time incurred due to actual identity theft; (h) failure to receive the benefit of the bargain when Defendant failed to provide adequate and reasonable protection that caused the Data Breach; (i) deprivation of value of PII/PHI; and (j) statutory damages.

6. Plaintiffs bring this class action against Defendant for its negligence, negligence

per se, breach of implied contract, violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq*. ("ICFA"), violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*. ("BIPA"), and unjust enrichment. Plaintiffs seek injunctive relief, declaratory relief, money damages, and all other relief as authorized in equity or by law.

THE PARTIES

7. Each Plaintiff is a citizen of Illinois with a residence in Cook County, Illinois.

8. Defendant is a professional limited liability company organized under Illinois law, with its principal place of business in Lake County, Illinois.

JURISDICTION AND VENUE

9. Subject matter jurisdiction arises under 28 U.S.C. § 1332(d). This is case is brought as a class action with an amount in controversy in excess of $5 million, exclusive of interest and costs, there are 100 or more proposed Class members, and at least one proposed Class member is a citizen of a state different from Defendant. Defendant's notice letter includes information expressly for residents of the District of Columbia, Maryland, New Mexico, New York, North Carolina, and Rhode Island, suggesting that Class members are citizens of different states from Defendant.

10. This Court has personal jurisdiction over Defendant because Defendant transacts business in Illinois, committed tortious acts in Illinois, contracted with Plaintiffs and Class members to provide reasonable data security in Illinois, is organized under the laws of Illinois, and has its principal place of business in Illinois and is at home in Illinois.

11. Venue is proper in this District because the acts and omissions giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

Defendant's Promises and Obligations Regarding Protection of PII/PHI

12. Defendant provides healthcare services to patients.

13. Plaintiffs and Class members obtained treatment from Defendant and were required to provide Defendant with their PII/PHI in the course of receiving treatment.

14. Plaintiffs and Class members relied on Defendant, a licensed medical treatment provider, to keep their PII/PHI confidential, secure, and to use it only for purposes of treatment and billing for authorized treatment, and to implement and follow adequate and reasonable data collection, storage, and retention policies. Defendant maintained and stored the PII/PHI on its systems and networks that were inadequately protected and ultimately accessed without authorization by criminals in the Data Breach.

15. Defendant owed Plaintiffs and Class members numerous statutory, regulatory, ethical, contractual, and common law duties to safeguard and keep Plaintiffs' and Class members' PII/PHI confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, and theft.

16. In its Privacy Policy, Defendant states that "We understand that your health information is personal, and are committed to protecting your privacy and ensuring that your health information is not used inappropriately."[1]

The Data Breach

17. Defendant's data breach notification letter states that on October 22, 2021, Defendant "discovered unusual activity within its computer network" caused by "malware" and launched an investigation. On November 18, 2021, Defendant's investigation determined that "on

[1] https://www.illinoisgastro.com/uploads/Notice_of_Privacy_Practices-3-13_2.pdf (last visited September 2, 2022).

or before October 20, 2021, an unauthorized actor gained access to certain IGG systems and that information contained in those systems may have been viewed or taken by the unauthorized actor." *See* Notice of Security Incident Letter, attached hereto as Exhibit 1.

18. The notice letter does not include details regarding the length of the Data Breach. According to the United States Department of Health and Human Services breach portal, the Data Breach resulted in the theft of PII/PHI of 227,943 patients.

19. On or about April 22, 2022, Defendant finally sent notification letters to Plaintiffs and Class members after failing to provide any notice to them for 5 months for no good reason.

20. In the notification, Defendant advises Plaintiffs and Class members to take steps to "protect your information." Defendant encourages Plaintiffs and Class members "to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credit reports for suspicious activity," and Defendant provides a document entitled "Steps You Can Take to Protect Personal Information." *See* Exhibit 1.

21. Currently, the full extent of the types of sensitive personal information, the scope of the Data Breach, and the details regarding how the Data Breach was carried out are all within the control of Defendant and its agents, counsel, and forensic security vendors at this phase of the litigation. However, in a separate notice regarding the Data Breach, Defendant stated that the following information maintained by Defendant in its systems was impacted in the Data Breach: name, address, date of birth, Social Security number, driver's license, Passport, financial account information, payment card information, employer-assigned identification number, medical information, and biometric data. *See* Defendant's Data Breach Notice, attached as Exhibit 2. Plaintiffs and Class members are aware that the type of data set published now provides a one-stop shop for identity thieves to wreak complete havoc on their lives. Given the sensitivity of the

information involved (such as Social Security numbers and medical information), Plaintiffs and Class members have all experienced a materialized and imminent risk of identity theft.

22. Cybersecurity experts have concluded that the kind of information taken in the Data Breach "would make it possible for malicious actors to carry out phishing attacks, social engineering, or even identity theft and bank fraud."[2]

23. The PII/PHI that was exfiltrated in the Data Breach was held in unencrypted form by Defendant, and included Plaintiffs' and Class members' PII/PHI.

The Data Breach Was Preventable

24. Defendant could have prevented the Data Breach by properly securing and encrypting the PII/PHI of Plaintiffs and Class members, by properly training its employees to recognize and prevent cybersecurity risks, and/or by implementing and following adequate procedures to monitor and detect data breaches. Defendant's negligence in safeguarding the PII/PHI of Plaintiffs and Class members was exacerbated by the repeated warnings and alerts directed to U.S. companies warning that they should protect and secure sensitive data, especially in light of the substantial increase in cyberattacks specifically targeting healthcare providers.

The Data Breach Was Foreseeable

25. The FBI has been warning healthcare providers, such as Defendant, about the threat posed by the ransomware and others, and to be on the lookout for attacks.

26. The United States Cybersecurity & Infrastructure Security Agency, Department of Justice, and Department of Health & Human Services issued a Joint Cybersecurity Advisory as early as on October 28, 2020, warning of an acute threat to U.S. hospitals and healthcare providers

[2] https://www.bleepingcomputer.com/news/security/engineering-firm-parker-discloses-data-breach-after-ransomware-attack/amp/ (last visited May 19, 2022).

and advising them on how to "ensure that they take timely and reasonable precautions to protect their networks from these threats."[3] The Advisory details at great length the pathways of specific viruses, malware, and online threats, and lists numerous Mitigation Steps, including:

- Patch operating systems, software, and firmware as soon as manufacturers release updates;
- Check configurations for every operating system version for organization-owned assets to prevent issues from arising that local users are unable to fix due to having local administration disabled;
- Regularly change passwords to network systems and accounts and avoid reusing passwords for different accounts;
- Use multi-factor authentication where possible;
- Disable unused remote access/remote desktop protocol (RDP) ports and monitor remote access/RDP logs;
- Implement application and remote access allow listing to only allow systems to execute programs known and permitted by the established security policy;
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind;
- Audit logs to ensure new accounts are legitimate;
- Scan for open or listening ports and mediate those that are not needed;
- Identify critical assets such as potential database servers, medical records,

[3] https://www.cisa.gov/uscert/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf (last visited July 20, 2022).

and telehealth and telework infrastructure; create backups of these systems and house the backups offline from the network;

- Implement network segmentation. Sensitive data should not reside on the same server and network segment as the email environment;
- Set antivirus and anti-malware solutions to automatically update; conduct regular scans.

27. In addition, the advisory emphasizes a focus on awareness and training. Because end users are targeted, employees need to be aware of threats and how they are delivered.

28. On information and belief, the hackers who carried out the Data Breach used rudimentary tactics for deploying malware on data rich systems, such as basic phishing emails. Such attacks are entirely preventable through proper training of employees to recognize phishing emails in combination with industry standard security measures such as required two-factor or multi-factor authentication to access email accounts and/or other computer systems.

29. Even with a successful initial infection vector through basic phishing techniques, the Data Breach could have been identified and halted quickly had Defendant implemented widely available software capable of fully detecting and preventing the Data Breach.

30. Despite the well-known risks and reasonable and effective protections, Defendant inexplicably failed to properly train employees, failed to implement industry standard security measures, and maintained highly sensitive patient information in a manner it knew or should have known was vulnerable to access and exfiltration.

31. Despite the prevalence of public announcements of these data breach and data security compromises and despite numerous attempts on the part of the federal government to inform companies like Defendant of the threats facing Defendant, and despite ample time to

implement precautions and training, Defendant was negligent and did not adequately prepare for this wholly foreseeable event.

32. As a result, Defendant allowed extremely sensitive data to be accessed, viewed and stolen by the criminals. Defendant breached its duty to take appropriate steps to protect Plaintiffs' and Class members' PII/PHI from being compromised and failed to adequately notify them that the Data Breach took place.

33. Unfortunately for Plaintiffs and Class members, their PII/PHI was not secured in the manner required by law that would have prevented the Data Breach.

34. What is worse, despite Defendant's obligations under the law to promptly notify affected individuals so they can take appropriate action, Defendant failed to promptly provide such notice in the most expedient time possible and without unreasonable delay, failed to include in the Data Breach notification letter a sufficient description of the Data Breach or the information needed by Plaintiffs and Class members to react appropriately to the Data Breach, including taking whatever mitigation measures are necessary.

35. As a result, this unauthorized access, disclosure, and exfiltration remains unremedied, and as detailed below the "cure" offered by Defendant to address these failures after the fact was wholly inadequate.

36. Defendant had specific obligations imposed on it by contracts and law to ensure the adequate protection of such information. For example, as a covered entity under HIPAA, Defendant was required to maintain the confidentiality and security of the PII/PHI of its patients.

Defendant's HIPAA Violations

37. Defendant is regulated by the Health Insurance Portability and Accountability Act ("HIPAA") (45 C.F.R. § 160.102), and is required to comply with the HIPAA Privacy Rule and

Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C, which establish national security standards and duties for Defendant's protection of medical information maintained in electronic form.

38. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

39. "Electronic protected health information" is defined as "individually identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

40. HIPAA's Security Rule requires Defendant to: (a) ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits; (b) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (c) protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and (d) ensure compliance by its workforce.

41. HIPAA also requires Defendant to "review and modify the security measures implemented ... as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(c), and also to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

42. The facts of the Data Breach establish that Defendant failed to comply with these Rules. The Data Breach resulted from a combination of inadequacies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations, including, but not limited to, the following:

(a) Failing to ensure the confidentiality and integrity of electronic PHI that Defendant creates, receives, maintains, and transmits, in violation of 45 C.F.R. section 164.306(a)(1);

(b) Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. section 164.312(a)(1);

(c) Failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. section 164.308(a)(1);

(d) Failing to identify and respond to suspected or known security incidents and mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. section 164.308(a)(6)(ii);

(e) Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. section 164.306(a)(2);

(f) Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding

individually identifiable health information, in violation of 45 C.F.R. section 164.306(a)(3);

(g) Failing to ensure compliance with HIPAA security standard rules by its workforce, in violation of 45 C.F.R. section 164.306(a)(4);

(h) Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. section 164.502, *et seq.*;

(i) Failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. sections 164.530(b) and 164.308(a)(5); and

(j) Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. section 164.530(c).

Defendant Violated Federal Trade Commission Guidelines

43. Defendant also violated the duties applicable to it under the Federal Trade Commission Act (15 U.S.C. § 45, *et seq.*) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC, pursuant to that Act, has concluded that a company's failure to maintain reasonable and appropriate data security for sensitive personal information is an "unfair practice" in violation of the FTC Act.

44. As established by these laws, Defendant owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and

protecting the medical information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant also owed a duty to Plaintiffs and Class members to provide reasonable security in compliance with industry standards and state and federal requirements, and to ensure that its computer systems, networks, and protocols adequately protected this medical information and were not exposed to infiltration. This also included a duty to Plaintiffs and Class members to design, maintain, and test its computer systems to ensure that the PII/PHI was adequately secured and protected; to create and implement reasonable data security practices and procedures to protect the PII/PHI through processes such as phishing, including adequately training employees and others who accessed information within its systems on how to adequately protect this information and avoid permitting such infiltration such as by use of multi-factor authentication; to implement processes that would detect a breach of its data security systems in a timely manner and to act upon data security warnings and alerts in a timely fashion; to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII/PHI from theft; and to disclose in a timely and accurate manner when data breaches occurred.

45. Defendant also needed to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems. It is apparent that Defendant did not do so.

46. Defendant owed these duties to Plaintiffs and Class members because they were foreseeable and probable victims of any inadequate data security practices. Defendant affirmatively chose to design these systems with inadequate user authentication, security protocols and privileges, and set up faulty patching and updating protocols. These affirmative decisions resulted in criminals successfully carrying out a cyberattack and exfiltrating Plaintiffs' and Class

members' PII/PHI, to the injury and detriment of Plaintiffs and Class members. By taking affirmative acts inconsistent with these obligations that left Defendant's computer systems foreseeably vulnerable to criminals, Defendant disclosed and/or permitted the disclosure of PII/PHI to unauthorized third parties. Defendant thus failed to preserve the confidentiality of PII/PHI it was duty-bound to protect.

Value of Personally Identifiable Information

47. The PII/PHI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[4] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[5] Criminals can also purchase access to entire company data breaches from $900 to $4,500.

48. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not

[4] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 17, 2022).

[5] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 17, 2022).

> find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[6]

49. It is incredibly difficult to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

50. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[7]

51. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft.

52. Indeed, a robust cyber black market exists in which criminals post stolen medical information, PII/PHI on multiple underground internet websites, commonly referred to as the dark web, to create fake insurance claims, purchase and resell medical equipment, or access prescriptions for illegal use or resale. According to a 2017 Javelin strategy and research presentation, fraudulent activities based on data stolen in data breaches that are between two and

---

[6] *Identity Theft and Your Social Security Number*, Social Security Administration, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 13, 2021).

[7] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Jan. 17, 2022).

six years old had increased by nearly 400% over the previous four years.[8] Thus, an offer of credit monitoring service that is only for one year is not an adequate remedy or offer, even if it conducts dark web scanning (which is unclear here).

53. According to Experian, one of the three major credit bureaus, medical records can be worth up to $1,000 per person on the dark web, depending upon completeness.[9] PII/PHI can be sold at a price ranging from approximately $20 to $300.[10]

54. In this case, all evidence indicates that Plaintiffs and Class members' PII/PHI was left unprotected, to be exfiltrated and sold on the dark web. Thus, this highly valuable data was left to be pilfered by criminals or reviewed by anyone with an Internet connection.

55. Medical identity theft can also result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences since if a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[11]

---

[8] *See,* Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web* (2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed 5/23/22).

[9] *Id.*

[10] https://www.privacyaffairs.com/dark-web-price-index-2021/

[11] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, (2/7/14), https://khn.org/news/rise-of-indentity-theft/ (last accessed 5/3/22); See also, Medical Identity Theft in the New Age of Virtual Healthcare, IDX (March 15, 2021), https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare (last accessed 5/3/22).

56. The Ponemon Institute found that medical identity theft can cost victims an average of $13,500 to resolve per incident, and that victims often have to pay off the imposter's medical bills to resolve the breach.[12]

57. In another study by the Ponemon Institute in 2015, 31% of medical identity theft victims lost their healthcare coverage as a result of the incident, while 29% had to pay to restore their health coverage, and over half were unable to resolve the identity theft at all.[13]

58. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, only credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach, including Social Security numbers and names, is impossible to "close" and difficult, if not impossible, to change.

59. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[14]

60. Among other forms of fraud, identity thieves may obtain driver's licenses,

[12] Brian O'Connor, Healthcare Data Breach: What to Know About Them and What to Do After One, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed 5/3/22).

[13] Ponemon Institute, Fifth Annual Study on Medical Identity Theft, (February, 2015), http://www.medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf (last accessed 5/3/22).

[14] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 17, 2022).

government benefits, medical services, and housing or even give false information to police.

61. The fraudulent activity resulting from the Data Breach may not come to light for years.

62. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII/PHI is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[15]

63. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII/PHI of Plaintiffs and Class members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class members as a result of a breach.

64. Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and the Class are incurring and will continue to incur such damages in addition to any fraudulent use of their PII/PHI.

65. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's storage platform, amounting to hundreds of thousands of individuals' detailed, personal information and, thus, the significant number of individuals who

[15] *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: https://www.gao.gov /assets/gao-07-737.pdf (last accessed Jan. 17, 2022).

would be harmed by the exposure of the unencrypted data.

66. To date, Defendant has offered Plaintiffs and Class members only one year of identity theft detection services. The offered service is wholly inadequate to protect Plaintiffs and Class members from the threats they face for years to come, particularly in light of the PII/PHI at issue here, and is not an adequate cure of the Data Breach.

67. Specifically, Defendant did not prevent the criminals from disclosing Plaintiffs' and Class members' PII/PHI on the Internet. Defendant has not and cannot retrieve the PII/PHI taken from its systems. Thus, that PII/PHI remains in circulation on the Internet for access, viewing, and misuse, causing damage to Plaintiffs and Class members and breaching their confidentiality.

68. Defendant has not provided sufficient information in its Data Breach notice letter such that Plaintiffs and Class members could understand and appreciate the full nature of the risk to them caused by Defendant's Data Breach, allowing them to make informed decisions about how to protect themselves and their PII/PHI.

69. Defendant has not provided credit monitoring and identity theft protection to Plaintiffs and Class members for a long enough period of time, limiting the bulk of the protection services to one year even though their PII/PHI may be used for years after that.

70. Defendant's offer of TransUnion credit monitoring and identity theft protection does not prevent fraudulent transactions, such as unauthorized credit card charges or exchanges of Plaintiffs' and Class members' PII/PHI on the dark web from occurring using the PII/PHI disclosed by Defendant. Neither can it prevent misuse of biometric information.

71. Additionally, Defendant has not taken the actions necessary and recommended by the FBI, CISA, NSA and other experts detailed above to prevent an attack by criminals, leaving

Plaintiffs and Class members vulnerable to subsequent breaches of their PII/PHI held by Defendant.

72. The injuries to Plaintiffs and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII/PHI of Plaintiffs and Class members.

PLAINTIFFS' EXPERIENCES

73. Plaintiffs each received healthcare from Defendant. As a condition of obtaining treatment, each Plaintiff provided their PII/PHI to Defendant with the reasonable expectation that Defendant would maintain such information in a secure manner, would implement reasonable data retention policies, and would only use their PII/PHI for legitimate business purposes.

74. Defendant expressly and impliedly promised to safeguard each Plaintiff's PII/PHI. Defendant assumed obligations to Plaintiffs, and Plaintiffs relied on Defendant to safeguard their PII/PHI and only to utilize it for legitimate business purposes. Defendant, however, did not take proper care of Plaintiffs' PII/PHI, leading to its exposure as a direct result of Defendant's inadequate security measures and negligent data retention policies. Had Plaintiffs known their PII/PHI would be insufficiently protected from known cyberthreats, Plaintiffs would not have disclosed the information to Defendant and would not have paid as much as they did for the healthcare services they bargained to receive—of which confidentiality was a material term.

75. On or about April 22, 2022, each Plaintiff received notice from Defendant that their PII/PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that each Plaintiffs' PII/PHI was accessed in the Data Breach.

76. As a result of the Data Breach, Plaintiffs made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing

financial, healthcare, and other accounts for any indications of actual or attempted identity theft or fraud. Plaintiffs have spent time and energy dealing with the Data Breach—valuable time Plaintiffs otherwise would have spent on other activities—including but not limited to work or recreation.

77. As a result of the Data Breach, Plaintiffs have suffered anxiety as a result of the release of their PII/PHI, which they reasonably believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using their PII/PHI for purposes of identity theft and fraud. Plaintiffs are very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

78. Plaintiffs suffered actual injury from having their PII/PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of PII/PHI, a form of property that Defendant obtained from Plaintiffs; (b) violation of privacy rights; (c) loss of the benefit of bargained for data security protections; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

79. As a result of the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiffs are at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS ACTION ALLEGATIONS

80. Plaintiffs seek to certify the following class pursuant to Fed. R. Civ. P. 23:

> All persons whose PII/PHI was accessed by unauthorized persons in the Data Breach.

81. Excluded from the Class are Defendant and Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives,

attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their immediate families, and members of their staff.

82. Plaintiffs reserve the right to amend or modify the Class definition and/or create additional subclasses as this case progresses.

83. Numerosity. The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class members is unknown to Plaintiffs at this time, Plaintiffs believe that the Class consists of approximately 227,943 persons based on Defendant's report to the Department of Health & Human Services.

84. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class members' PII/PHI;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class members to safeguard their PII/PHI;

f. Whether Defendant breached its duty to Class members to safeguard their PII/PHI;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein breached express or implied contracts with Plaintiffs and Class members;

l. Whether Defendant violated the Illinois Consumer Fraud and Deceptive Business Practices Act;

m. Whether Defendant violated the Illinois Biometric Information Privacy Act;

n. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon it by Plaintiffs and Class members; and;

o. Whether Plaintiffs and Class members are entitled to damages, punitive damages, treble damages, statutory damages, and/or injunctive or other equitable relief.

85. Typicality. Plaintiffs' claims are typical of those of other Class members because Plaintiffs' information, like that of every other Class member, was compromised in the Data Breach.

86. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' counsel is competent and experienced in litigating class actions.

87. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class members, in that all of Plaintiffs' and Class members' PII/PHI was stored on the same computer network and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

88. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

89. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

90. Plaintiffs re-allege and incorporate by reference paragraphs 1–89 as if fully set forth herein.

91. As a condition of obtaining treatment, Plaintiffs and Class members provided Defendant with their PII/PHI.

92. Plaintiffs and Class members entrusted their PII/PHI to Defendant with the understanding and relying upon Defendant to exercise reasonable care in the protection of their PII/PHI.

93. Defendant had a duty to take reasonable measures to protect the PII/PHI of Plaintiffs and Class members from unauthorized disclosure to third parties. This duty is inherent in the nature of the exchange of highly sensitive personal information in connection with the patient-physician relationship.

94. Defendant has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiffs and Class members could and would suffer if the PII/PHI were wrongfully disclosed in a Data Breach.

95. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, using, and retaining of the PII/PHI of Plaintiffs and Class members, without adequate data security, involved an unreasonable risk of harm to Plaintiffs and Class members.

96. Defendant had a duty to exercise reasonable care in safeguarding, securing, retaining, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, design, configuring,

maintaining, and testing Defendant's security protocols to ensure that the PII/PHI of Plaintiffs and Class members in Defendant's possession was adequately secured and protected.

97. Defendant also had a duty to exercise appropriate practices to remove PII/PHI that was no longer required.

98. Defendant had a duty to encrypt the sensitive PII/PHI it stored and maintained.

99. Defendant had a duty to segregate sensitive PII/PHI from other portions of its network, such as by using firewalls.

100. Defendant had a duty to properly train employees to recognize phishing attempts and other common data security risks.

101. Defendant also had a duty to implement and maintain procedures to detect and prevent the improper access, exfiltration, and misuse of PII/PHI.

102. Defendant's duty to use reasonable security measures arose as a result of the relationship that existed between Defendant and Plaintiffs and Class members. Plaintiffs and Class members entrusted Defendant with their confidential PII/PHI and relied upon Defendant to implement adequate data security and reasonable data retention policies.

103. Defendant was subject to an independent duty arising out of the common law between Defendant and Plaintiffs or Class members.

104. A breach of security, unauthorized access, and resulting injury to Plaintiffs and Class members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices, the detailed warnings published by governmental agencies, and news reports of other data breaches.

105. Plaintiffs and Class members were the foreseeable and probable victims of Defendant's inadequate and unreasonable data security practices and procedures. Defendant knew

or should have known of the inherent risks in collecting and storing the PII/PHI, the critical importance of providing adequate security of that PII/PHI, the necessity for encrypting PII/PHI, and the harm that can arise from retaining PII/PHI following the expiration of any legitimate business purpose.

106. Defendant's conduct created a foreseeable risk of harm to Plaintiffs and Class members. Defendant solicited, collected, digitized, and aggregated Plaintiffs' and Class members' PII/PHI, failed to encrypt the PII/PHI, failed to implement other reasonable industry standard measures to safeguard PII/PHI, and failed to implement retention policies that delete PII/PHI.

107. Plaintiffs and Class members had no ability to protect their PII/PHI that was in, and remains in, Defendant's possession, and no sign that Defendant was failing and refusing to implement and maintain reasonable data security practices over their PII/PHI until they received their notification letters.

108. Defendant was in a position to protect against the harm suffered by Plaintiffs and Class members as a result of the Data Breach.

109. Defendant had and continues to have a duty to adequately disclose that the PII/PHI might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice is necessary to allow Plaintiffs and the Class members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII/PHI.

110. Defendant had a duty to employ proper procedures to prevent the unauthorized disclosure and unauthorized sharing of the PII/PHI to criminals.

111. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class members by failing to implement and maintain industry-standard protocols

and to exercise reasonable care in protecting and safeguarding the PII/PHI of Plaintiffs and Class members.

112. Defendant improperly and inadequately safeguarded the PII/PHI of Plaintiffs and Class members in violation of standard industry rules, regulations, and practices at the time of the Data Breach.

113. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class members by failing to have appropriate procedures in place to detect and prevent unauthorized dissemination of PII/PHI.

114. Defendant breached its duty to remove PII/PHI that it was no longer required to retain pursuant to regulations.

115. Defendant breached its duty to encrypt PII/PHI and to segregate it from other portions its network.

116. Defendant breached its duty to adequately train employees to recognize and avoid phishing attempts and other basic cybersecurity risks.

117. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and Class members the existence and scope of the Data Breach.

118. Defendant breached its duty to safeguard Plaintiffs' and Class members' PII/PHI by failing to retain such information in an encrypted form.

119. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class members, the PII/PHI of Plaintiffs and Class members would not have been compromised.

120. There is a close causal connection between Defendant's failure to implement security measures to protect the PII/PHI of Plaintiffs and Class members and the harm, or risk of

imminent harm, suffered by Plaintiffs and Class members. The PII/PHI of Plaintiffs and Class members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII/PHI by adopting, implementing, and maintaining appropriate security measures.

121. As a direct and proximate result of Defendant's numerous negligent acts and omissions, Plaintiffs and Class members are at a substantial, impending, and imminent risk of identity theft, and they have been forced to take mitigation steps, thereby incurring costs, to ensure their personal and financial safety.

122. As Defendant instructed, advised, and warned in its notice letters, Plaintiffs and Class members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiffs and Class members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included, and will include into the future, protective steps: *e.g.*, reviewing financial statements, changing passwords, and signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

123. As a direct and proximate result of Defendant's numerous negligent acts and omissions, Plaintiffs and Class members have suffered actual and concrete injuries and will suffer addition injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (d) loss of time and loss of productivity heeding Defendant's warnings and following its instructions in the notice letter; (e) financial costs incurred due to actual identity theft; (f) the cost

of future identity theft monitoring; (g) loss of time incurred due to actual identity theft; (h) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; and (i) and diminution of value of their PII/PHI.

124. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their PII/PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI in its continued possession. Plaintiffs and Class members are, therefore, also seeking injunctive relief for the continued risk to their PII/PHI, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to safeguard the PII/PHI.

125. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class members are entitled to recover actual and punitive damages.

COUNT II
Negligence *per se*
(On Behalf of Plaintiffs and the Class)

126. Plaintiffs re-allege and incorporate by reference paragraphs 1–89 as if fully set forth herein.

127. Defendant violated HIPAA regulations, including by:

- Failing to ensure the confidentiality and integrity of electronic PHI that Defendant creates, receives, maintains, and transmits, in violation of 45 C.F.R. section 164.306(a)(1);
- Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to

those persons or software programs that have been granted access rights, in violation of 45 C.F.R. section 164.312(a)(1);

- Failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. section 164.308(a)(1);
- Failing to identify and respond to suspected or known security incidents and mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. section 164.308(a)(6)(ii);
- Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. section 164.306(a)(2);
- Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. section 164.306(a)(3);
- Failing to ensure compliance with HIPAA security standard rules by its workforce, in violation of 45 C.F.R. section 164.306(a)(4);
- Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. section 164.502, *et seq.*;
- Failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI

as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. sections 164.530(b) and 164.308(a)(5); and,

- Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. section 164.530(c).

128. "Section 5 of the FTC Act [15 U.S.C. § 45] is a statute that creates enforceable duties, and this duty is ascertainable as it relates to data breach cases based on the text of the statute and a body of precedent interpreting the statute and applying it to the data beach context." *In re Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407 (E.D. Va. 2020). "For example, in *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015), the United States Court of Appeals for the Third Circuit affirmed the FTC's enforcement of Section 5 of the FTC Act in data breach cases." *Capital One*, 488 F. Supp. 3d at 407.

129. Plaintiffs' and Class members' PII/PHI was and is nonpublic personal information and customer information.

130. Plaintiffs and Class members are in the group of persons that HIPAA and the FTC Act were enacted and implemented to protect, and the harms they suffered in the Data Breach as a result of Defendant's violations of HIPAA and the FTC Act were the types of harm the statutes and regulations are designed to prevent.

131. As a direct and proximate result of Defendant's numerous negligent acts and omissions, Plaintiffs and Class members are at a substantial, impending, and imminent risk of identity theft, and they have been forced to take mitigation steps, thereby incurring costs, to ensure their personal and financial safety.

132. As a direct and proximate result of the conduct of Defendant that violated HIPAA and the FTC Act, Plaintiffs and Class members have suffered and will continue to suffer the foreseeable economic and non-economic harms as described herein.

133. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class members are entitled to recover actual and punitive damages.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

134. Plaintiffs re-allege and incorporate by reference paragraphs 1–89 as if fully set forth herein.

135. Defendant required Plaintiffs and Class members to provide their PII/PHI as a condition of receiving treatment. In so doing, Plaintiffs and Class members entered into implied contracts with Defendant wherein Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class members if their PII/PHI had been breached and compromised or stolen.

136. Defendant further entered into an implied contract with Plaintiffs and the Class members to honor its representations and assurances regarding protecting their PII/PHI.

137. Plaintiffs and Class members fully performed their obligations under implied contracts with Defendant.

138. Defendant breached the implied contracts it made with Plaintiffs and Class members by (i) failing to implement technical, administrative, and physical security measures to protect the PII/PHI from unauthorized access or disclosure (such as encryption of Social Security numbers) despite such measures being readily available, (ii) failing to limit access to the PII/PHI

to those with legitimate reasons to access it, (iii) failing to store the PII/PHI only on servers kept in a secure, restricted area, and (iv) otherwise failing to safeguard the PII/PHI.

139. As a direct and proximate result of Defendant's breach of its implied contract, Plaintiffs and Class members are at a substantial, impending, and imminent risk of identity theft, and they have been forced to take mitigation steps, thereby incurring costs, to ensure their personal and financial safety.

140. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and Class members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic damages in the following forms: (a) financial costs incurred mitigating the imminent risk of identity theft; (b) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity heeding Defendant's warnings and following its instructions in the notice letter; (d) financial costs incurred due to actual identity theft; (e) the cost of future identity theft monitoring; (f) loss of time incurred due to actual identity theft; (g) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls, (h) failure to receive the benefit of their bargained for data protection for which Plaintiffs and Class members paid a premium to Defendant; and (i) diminution of value of their PII/PHI.

141. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class members are entitled to recover actual, consequential, and nominal damages.

COUNT IV
Violation of Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq*.
(On Behalf of Plaintiffs and the Class)

142. Plaintiffs re-allege and incorporate by reference paragraphs 1–89 as if fully set forth herein.

143. As a corporation that collects, handles, stores, and maintains patient information that is nonpublic and personally identifiable information, Defendant is a data collector within the meaning of 815 ILCS 530/5.

144. As a data collector, Defendant is required to implement and maintain reasonable security measures to protect Plaintiffs' and Class members' PII/PHI from unauthorized access, acquisition, destruction, use, modification, or disclosure. 815 ILCS 530/45.

145. Defendant breached these duties and the applicable standards of care by:

- Failing to conduct proper and reasonable due diligence and oversight over employees, agents, and vendors who access to PII/PHI and their data security systems, practices, and procedures;
- Failing to conduct proper and reasonable due diligence over the employees, agents, and vendors who were the vector(s) of and/or facilitated the hackers' infiltration into the system(s) storing Plaintiffs' and Class members';
- Failing to maintain reasonable and appropriate oversight and audits on employees, agents, or vendors who were the vectors of the hackers' infiltration into the system(s) storing Plaintiffs' and Class members' PII/PHI;

- Failing to implement and maintain reasonable safeguards and procedures, such as encryption, to prevent the unauthorized disclosure of Plaintiffs' and Class members' PII/PHI;
- Failing to monitor and detect its confidential and sensitive data environment(s) storing Plaintiffs' and Class members' PII/PHI reasonably and appropriately in order to repel or limit the Data Breach;
- Failing to implement and maintain reasonable data storage and retention procedures with respect to the PII/PHI to ensure the PII/PHI was being stored and maintained for legitimate and useful purposes;
- Failing to undertake reasonable and sufficient incident response measures to ensure that the cyberattack directed toward Defendant's sensitive information would be thwarted and not expose and cause disclosure and unauthorized acquisition of Plaintiffs' and Class members' PII/PHI;
- Failing to cure deficiencies in data security that allowed the Data Breach to continue, grow in severity and scope, and go undetected and undeterred for additional time;
- Failing to ensure that Plaintiffs' and Class members' PII/PHI was timely deleted, destroyed, rendered unable to be used, or returned to Plaintiffs and Class members;
- Failing to reasonably conduct a forensic investigation into the scope, nature, and exposure of the Data Breach or to ascertain its full severity;
- Failing to provide full disclosure about, and deceptively misleading consumers through false representations and misleading omissions of fact

regarding, the Data Breach, consumers' risk and exposure caused by the Data Breach, and the adequacy of the investigation of and response to the Data Breach;

- Failing to provide accurate, complete, and sufficiently detailed notification to Plaintiffs and Class members regarding the circumstances of the Data Breach, its causes, its effects, the extent of the exposure of their PII/PHI, and details regarding the disposition of Plaintiffs' and the other Class members' PII/PHI at all times during the Data Breach.

146. Defendant failed to timely notify Plaintiffs and Class members that their PII/PHI was acquired in the Data Breach. Defendant waited 5 months to mail a letter to Plaintiffs and Class members. Defendant had all the information it needed to disseminate notification to Plaintiffs and the other Class members on November 18, 2021, when Defendant's investigation determined that the Data Breach occurred on or before October 20, 2021. Likely, notification could have been provided in mere days to all the individuals whose names and information was contained in the files that were accessed by the criminals. Instead, Defendant delayed notification while cyber criminals were able to perpetrate fraud with Plaintiffs' and Class members' PII/PHI unbeknownst to them for an additional 5 months after Defendant confirmed the existence of the Data Breach.

147. As a proximate result of Defendant's unfair acts and practices described above and the resulting injuries to Plaintiffs and Class members, as herein alleged, Plaintiffs and Class members have incurred damages.

148. As a direct and proximate result of Defendant's unlawful acts and omissions, Plaintiffs and Class members have suffered actual and concrete injuries and will suffer addition injuries into the future, including economic and non-economic damages in the following forms:

(a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (d) loss of time and loss of productivity heeding Defendant's warnings and following its instructions in the notice letter; (e) financial costs incurred due to actual identity theft; (f) the cost of future identity theft monitoring; (g) loss of time incurred due to actual identity theft; (h) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; and (i) and diminution of value of their PII/PHI.

149. Additionally, as a direct and proximate result of Defendant's unlawful conduct, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their PII/PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI in its continued possession. Plaintiffs and Class members are, therefore, also seeking injunctive relief for the continued risk to their PII/PHI, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to safeguard the PII/PHI.

150. As a direct and proximate result of Defendant's unlawful conduct, Plaintiffs and Class members are entitled to recover actual, consequential, punitive damages, as well as injunctive relief, and reasonable attorney's fees and costs, pursuant to 815 ILCS 505/10a and 815 ILCS 505/2z.

COUNT V
Violation of Illinois Biometric Information Privacy Act
740 ILCS 14/1, *et seq*. ("BIPA")
(On Behalf of Plaintiffs and the Class)

151. Plaintiffs re-allege and incorporate by reference paragraphs 1–89 as if fully set forth herein.

152. Defendant is a "private entity" within the meaning of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1.

153. Defendant collected and stored Plaintiffs' and Class members private biometric identifiers.

154. Defendant violated 740 ILCS 14/15(d) by failing to obtain consent to the disclosure of Plaintiffs' and Class members' private biometric identifiers and biometric information in the Data Breach.

155. Defendant violated 740 ILCS 14/15(e) by failing to store, transmit, and protect from disclosure all biometric identifiers and biometric information of Plaintiffs and Class members using a reasonable standard of care within Defendant's industry in the Data Breach.

156. Defendant's conduct in violation of the BIPA was negligent, reckless, and intentional.

157. As a proximate result of Defendant's unfair acts and practices described above and the resulting injuries to Plaintiffs and Class members, as herein alleged, Plaintiffs and Class members have incurred damages.

158. As a direct and proximate result of Defendant's unlawful acts and omissions, Plaintiffs and Class members have suffered actual and concrete injuries and will suffer addition injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (d) loss of time and loss of productivity heeding Defendant's warnings and following its instructions in the notice letter; (e) financial costs incurred due to actual identity theft; (f) the cost of future identity theft monitoring; (g) loss of time incurred due to actual identity theft; (h) loss of time and

annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; and (i) and diminution of value of their PII/PHI.

159. Additionally, as a direct and proximate result of Defendant's unlawful conduct, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their PII/PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI in its continued possession. Plaintiffs and Class members are, therefore, also seeking injunctive relief for the continued risk to their PII/PHI, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to safeguard the PII/PHI.

160. Plaintiffs and Class members seek injunctive and equitable relief; statutory damages of $1,000 per violation for each of Defendant's negligent violations of BIPA and $5,000 for each intentional violation of BIPA; and reasonable attorneys' fees and costs and expenses pursuant to 740 ILCS 14/20.

COUNT VI
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

161. Plaintiffs re-allege and incorporate by reference paragraphs 1–89 as if fully set forth herein.

162. This claim is brought in the alternative to Plaintiffs' other claims at law.

163. Defendant benefited from receiving Plaintiffs' and Class members' PII/PHI by its ability to retain and use that information for its own benefit.

164. Defendant also understood and appreciated that Plaintiffs' and Class members' PII/PHI was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

165. Plaintiffs and Class members conferred a benefit upon Defendant by paying for its services, and in connection therewith, by providing their PII/PHI to Defendant with the understanding that Defendant would implement and maintain reasonable data privacy and security practices and procedures. Plaintiffs and Class members should have received adequate protection and data security for such PII/PHI held by Defendant.

166. Defendant knew Plaintiffs and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and appreciated the benefits.

167. Defendant failed to provide reasonable security, safeguards, and protections to the PII/PHI of Plaintiffs and Class members.

168. Defendant should not be permitted to retain money rightfully belonging to Plaintiffs and Class members, because Defendant failed to implement appropriate data security measures and caused the Data Breach.

169. Defendant accepted and wrongfully retained these benefits to the detriment of Plaintiffs and Class members.

170. Defendant's enrichment at the expense of Plaintiffs and Class members is and was unjust.

171. As a result of Defendant's wrongful conduct, as alleged above, Plaintiffs and Class members seek restitution of their money paid to Defendant, and disgorgement of all profits, benefits, imposition of a constructive trust, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class, pray for judgment against Defendant and in Plaintiffs' favor, as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

b) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

c) For an award of punitive damages, as allowable by law;

d) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

e) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' PII/PHI, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class members;

f) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII/PHI compromised during the Data Breach;

g) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

h) Imposition of a constructive trust for the benefit of Plaintiffs and Class members;

i) Pre- and post-judgment interest on any amounts awarded; and,

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Plaintiffs MEYER GELFMAN, BORIS PARAD, and YELENA PARAD, individually, and on behalf of all others similarly situated,

By: */s/ Thomas A. Zimmerman, Jr.*

Thomas A. Zimmerman, Jr.
Jeffrey D. Blake
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
Phone: (312) 440-0020
Fax: (312) 440-4180
tom@attorneyzim.com
www.attorneyzim.com

Counsel for Plaintiffs and the Class

Illinois Gastroenterology Group
IGG
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

400570430000857939
000 0008661 00000000 0001 0002 04331 INS: 0 0

BORIS PARAD
[redacted]

April 22, 2022

NOTICE OF SECURITY INCIDENT

Dear Boris Parad:

Illinois Gastroenterology Group, PLLC ("IGG") is writing to inform you of an event that may impact the security of some of your information. Although we have received no indication of any actual or attempted misuse of your information as a result of this event, this notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it is necessary to do so.

What Happened? On October 22, 2021, IGG discovered unusual activity within its computer network. IGG immediately launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. On November 18, 2021, the investigation determined that on or before October 20, 2021, an unauthorized actor gained access to certain IGG systems and that information contained in those systems may have been viewed or taken by the unauthorized actor.

Therefore, we reviewed the information within those systems to identify if any individuals' personal information or protected health information was potentially accessible. On March 22, 2022, we discovered that your information was impacted as a result of this event. Although we are unaware of any actual or attempted misuse of your personal information, we are providing you this notice out of an abundance of caution.

What Information Was Involved? The investigation determined that your name, address, and medical information may have been accessible.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon learning of the event, we moved quickly to investigate and respond to the event, assess the security of our systems, and notify potentially affected individuals. In order to mitigate harm and protect against further incidences, IGG immediately engaged a leading cybersecurity forensics firm to work with internal teams to thoroughly investigate our networks and remove any indication of malware. Additionally, IGG's IT Department accelerated the implementation of an enhanced managed Security Operations Center, including the deployment of an endpoint detection and response platform in response to this event. Employee user accounts passwords were immediately reset and employees with privileged access to sensitive systems were enrolled into a multifactor authentication platform. IGG's sensitive system logs are monitored with threat signatures, which are updated continually for indications of malware.

We are also notifying potentially affected individuals, including you, so that you may take further steps to best protect your information, should you feel it is necessary to do so. We regret any inconvenience or concern this event may cause. As an added precaution, and although we do not have any indication of any actual or attempted misuse of your personal information, we are offering credit monitoring and identity theft protection services, through TransUnion, for 12 months at no cost to you.

EXHIBIT 1

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credit reports for suspicious activity and to report any suspicious activity promptly to your bank or financial institution. Additional information and resources are included in the enclosed *Steps You Can Take To Protect Personal Information*. You may also enroll in the complimentary credit monitoring services available to you. Enrollment instructions are attached to this letter.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at 1-833-559-1331, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays. Again, we take the privacy and security of information in our care very seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,

Illinois Gastroenterology Group, PLLC

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

Activation Code: FGMPDBHPBVPZ

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for 12 months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code **FGMPDBHPBVPZ** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code **699784** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain 12 months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *my*TrueIdentity online Credit Monitoring service anytime between now and **July 31, 2022**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *my*TrueIdentity online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, explanation of benefits forms and to monitor your credit reports for suspicious activity. Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. IGG is located at Illinois Gastroenterology Group, PLLC, Attention: Chief Operating Officer, P.O. Box 7630, Gurnee, IL 60031.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 9 Rhode Island residents impacted by this incident.

Illinois Gastroenterology Group, PLLC Provides Notice of a Security Incident

Illinois Gastroenterology Group, PLLC ("IGG") is providing notice of a recent incident that may affect the security of certain individuals' information.

What Happened? On October 22, 2021, IGG discovered unusual activity within its computer network. IGG immediately launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. On November 18, 2021, the investigation determined that an unauthorized actor gained access to certain IGG systems and that information contained in those systems may have been viewed or taken by the unauthorized actor.

Although there is no indication that identity theft or fraud occurred as a result of this incident, IGG has not been able to rule out the possible that some individuals' information was or may have been viewed or taken. Therefore, in an abundance of caution, IGG reviewed the information contained within the systems to identify if any individuals' personal information or protected health information was potentially impacted. On March 22, 2022, the review determined that certain information related to individuals was or may have been impacted.

What Information was Involved? The following types of information that IGG maintains in its systems and that were, or may have been, impacted by this incident include: name, address, date of birth, Social Security number, driver's license, Passport, financial account information, payment card information, employer-assigned identification number, medical information, and biometric data. To date, IGG has not received any reports of fraudulent misuse of any information potentially impacted.

What is IGG Doing? IGG takes this incident and the security of personal information in its care seriously. IGG moved quickly to investigate and respond to this incident, assess the security of its systems, and notify potentially affected individuals. In response to this incident, IGG augmented its policies and procedures addressing network security. IGG accelerated the implementation of an enhanced managed Security Operations Center including the deployment of an endpoint detection and response platform in response to this event with policies enabled specially for ransomware. IGG immediately reset passwords and employees with privileged access to sensitive systems were enrolled into our multifactor authentication platform. IGG is also notifying potentially affected individuals so that they may take further steps to protect their information, should they feel it is appropriate to do so.

What Can Impacted Individuals Do? IGG established a dedicated assistance line for individuals seeking information regarding this incident. Individuals seeking additional information may call the toll-free assistance line at 1-833-559-1331. This toll-free number is available Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays. Individuals may also write to IGG at Illinois Gastroenterology Group, PLLC, Attention: Chief Operating Officer, P.O. Box 7630, Gurnee, IL 60031.

Potentially affected individuals may also consider the information and resources outlined below. IGG encourages potentially impacted individuals to remain vigilant against identity theft and fraud by reviewing their account statements, credit reports, and explanation of benefits forms for suspicious activity and to report any suspicious activity promptly to their bank, financial institution, insurance company, health care provider, law enforcement, or their state Attorney General.

Steps You Can Take To Protect Your Personal Information

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit

www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If an individual is the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should they wish to place a fraud alert, they may contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in an individual's name without their consent. However, individuals should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, an individual cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals will need to provide the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should individuals wish to place a credit freeze, they may contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Individuals may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General.

The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal

Trade Commission also encourages those who discover that their information has been misused to file a complaint with it. Individuals can obtain further information on how to file such a complaint by way of the contact information listed above. Individuals have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, individuals will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and their state Attorney General. This notice has not been delayed by law enforcement.